中華民國經濟部智慧財產局

INTELLECTUAL PROPERTY OFFICE
MINISTRY OF ECONOMIC AFFAIRS
REPUBLIC OF CHINA

茲證明所附文件，係本局存檔中原申請案的副本，正確無訛，
其申請資料如下 ：

This is to certify that annexed is a true copy from the records of this office of the application as originally filed which is identified hereunder：

申　請　日：西元 2003 年 07 月 07 日
Application Date

申 請 案 號：092118467
Application No.

申　請　人：凌陽科技股份有限公司
Applicant(s)

局　　長
Director General

蔡練生

發文日期：西元 2004 年 3 月 25 日
Issue Date

發文字號：09320286160
Serial No.

發明專利說明書

（填寫本書件時請先行詳閱申請書後之申請須知，作※記號部分請勿填寫）

※ 申請案號：92118467　※IPC分類：

※ 申請日期：92.7.07

壹、發明名稱

（中文）於處理器中使用位址線對資料進行混淆處理的裝置及方法

（英文）

貳、發明人（共 1 人）

發明人 1 （如發明人超過一人，請填說明書發明人續頁）

姓名：（中文）梁伯嵩

（英文）

住居所地址：（中文）高雄市左營區裕誠路 406 號 6 樓之 1

（英文）

國籍：（中文）中華民國　（英文）

參、申請人（共 1 人）

申請人 1 （如發明人超過一人，請填說明書申請人續頁）

姓名或名稱：（中文）凌陽科技股份有限公司

（英文）

住居所或營業所地址：（中文）新竹縣科學園區創新一路 19 號

（英文）

國籍：（中文）中華民國　（英文）

代表人：（中文）黃洲杰

（英文）

☐ 續發明人或申請人續頁 （發明人或申請人欄位不敷使用時，請註記並使用續頁）

肆、中文發明摘要

本發係提出一種於處理器中使用位址線對資料進行混淆處理的裝置及方法，其包含一種子產生裝置、一第一參數產生裝置、一資料混淆處理裝置及一資料反混淆處理裝置。種子產生裝置係耦合至位址匯流排，以依據位址匯流排上之特定位址而產生一種子，第一參數產生裝置係耦合至種子產生裝置，以依據該種子產生一第一參數，資料混淆處理裝置其耦合至資料匯流排，以當處理器核心欲寫出資料至特定位址時，依據第一參數而對資料進行混淆處理，資料反混淆處理裝置其耦合至資料匯流排，以當處理器核心欲由特定位址讀入資料時，依據第一參數而對該資料進行反混淆處理。

伍、英文發明摘要

陸、(一)、本案指定代表圖爲：圖 2

(二)、本代表圖之元件代表符號簡單說明：

處理器核心	200	位址匯流排	210
資料匯流	220	種子產生裝置	230
第一參數產生裝置	240	資料混淆處理裝置	250
資料反混淆處理裝置	260	選擇裝置	271
選擇裝置	272	第二參數產生裝置	280
記憶體	290		

柒、本案若有化學式時，請揭示最能顯示發明特徵的化學式：

捌、聲明事項

☐ 本案係符合專利法第二十條第一項□第一款但書或□第二款但書規定之期間，其日期為：＿＿＿＿＿＿＿＿＿＿

☐ 本案已向下列國家（地區）申請專利，申請日期及案號資料如下：

【格式請依：申請國家（地區）；申請日期；申請案號　順序註記】

1. 無
2.
3.

☐ 主張專利法第二十四條第一項優先權：

【格式請依：受理國家（地區）；日期；案號　順序註記】

1.
2.
3.
4.
5.
6.
7.
8.
9.
10.

☐ 主張專利法第二十五條之一第一項優先權：

【格式請依：申請日；申請案號　順序註記】

1.
2.
3.

☐ 主張專利法第二十六條微生物：

☐國內微生物　【格式請依：寄存機構；日期；號碼　順序註記】

1.
2.
3.

☐國外微生物　【格式請依：寄存國名；機構；日期；號碼　順序註記】

1.
2.
3.

☐熟習該項技術者易於獲得，不須寄存。

玖、發明說明

（發明說明應敘明：發明所屬之技術領域、先前技術、內容、實施方式及圖式簡單說明）

【一、發明所屬之技術領域】

本發明係關於處理器的技術領域，尤指一種於處理器中使用位址線對資料進行混淆處理的裝置及方法。

【二、先前技術】

在這重視智財權的時代，廠商為了保護其辛苦開發之程式、資料等相關的智慧財產，會於離線(off-line)時將該等資料、程式先進行一混淆(scrambling)處理，再將混淆後的資料予以儲存至一非揮發性記憶體或其他儲存媒體，他人即使拿到存有該混淆資料的非揮發性記憶體或其他儲存媒體，由於無法知道該混淆處理之過程及處理方法，亦無法正確去還原該等資料、程式，藉此而達到保護之目的。

針對此種資料保護方式，於美國第USP6,408,073號專利案公告中，使用一虛擬亂數產生器(Pseudo Random Generator)，以依據一初始值(seed1/seed2)來對唯讀記憶體(Read Only Memory，ROM)之資料(ROM data)進行編碼以產生編碼資料(Encoded data)，然而此種資料保護方式因使用亂數做混淆處理之參數，需有同步之亂數產生器用以進行解碼，而亂數產生與執行順序相關，因為的執行有一定順序，故只能循序讀出，不能隨機讀出，難以應付程式執行中動態分支跳躍，因此不能直接在此ROM上執行程式，圖1即顯示一段程式碼，其程式碼事先利用

亂數順序以加密後儲存於一ROM，該段程式碼所儲存的位址係由1F00_0000$_H$至1F00_0020$_H$，若一處理器直接執行此段程式碼，會在條件式分支上出現問題，例如當該處理器執行到位於1F00_000C之指令#3時，若指令#3為bz 1F00_0020$_H$，此時若根據零旗標(zero flag)的值，決定該處理器跳躍到1F00_0020$_H$位址處繼續執行，此時會產生一問題，因為1F00_0020$_H$位址處所儲存之資料係將指令#8用虛擬亂數產生器(Pseudo Random Generator)所產生之一數值78編碼後的結果，可是虛擬亂數產生器此時產生的卻是60，而該處理器採用60來對儲存於1F00_0020$_H$位址處之資料做解碼，會產生錯誤而無法正確執行，甚至會使該處理器當機，因此，採用亂數產生器或虛擬亂數產生器來做混淆處理僅能用於固定的循序資料讀取的保護，不能用於儲存在ROM、RAM或Flash等記憶體中可執行程式之資料保護。

針對採用亂數產生器或虛擬亂數產生器來做混淆處理僅能用固定的循序資料讀取之限制，於美國第USP5,943,283號專利案公告中，係使用一位址混淆處理裝置以將順序之輸入位址轉換成非順序之實際位址，而達到對儲存在RAM或Flash等隨機讀存記憶體之資料的保護，然而此種資料保護方法中，若儲存的有某段資料本身有明顯易見的順序性(如處理器的啟動(Boot-up Strap)程序，或是常用的函數表格)，容易由資料排列位置方式猜出所使用混淆處理方法而被破解，因此，習知

資料之混淆處理方法的設計仍有諸多缺失而有予以改進之必要。

發明人爰因於此，本於積極發明之精神，亟思一種可以解決上述問題之「使用位址線對資料進行混淆處理的處理器及其方法」，幾經研究實驗終至完成此項發明。

〖三、發明內容〗

本發明之目的係在提供一種於處理器中使用位址線對資料進行混淆處理的裝置及方法，以避免習知技術僅能用於ROM的固定循序資料讀取資料的保護，而能用於如RAM或Flash等隨機讀存記憶體之資料保護。

依據本發明之一特色，係提出一種於處理器中使用位址線對資料進行混淆處理的裝置，該處理器具有一處理器核心以執行該處理器之相關指令，並利用一位址匯流排及資料匯流排以存取資料，該裝置包含一種子產生裝置、一第一參數產生裝置、一資料混淆處理裝置及一資料反混淆處理裝置。該種子產生裝置係耦合至該位址匯流排，以依據該位址匯流排上之特定位址而產生一種子；該第一參數產生裝置係耦合至該種子產生裝置，以依據該種子產生一第一參數；該資料混淆處理裝置其耦合至該資料匯流排，以當該處理器核心欲寫出資料至特定位址時，依據該第一參數而對該資料進行混淆處理；該資料反混淆處理裝置其耦合至該資料匯流排，以當該處理器核心欲由特定位址讀入資料時，依據該第一參數而對該資料進行反混淆處理。

依據本發明之另一特色，係提出一種於一處理器中使用位址線對資料進行混淆處理的方法，該處理器包含一處理器核心，該處理器核心係執行該處理器之相關指令，並利用一位址匯流排及第一資料匯流排以存取資料，該方法包含：一種子產生步驟，係依據該位址匯流排上之特定位址以產生一種子；一第一參數產生步驟，係依據該種子而產生一第一參數；一資料混淆處理步驟，依據該第一參數以對該處理器核心欲寫出至特定位址之資料進行混淆處理；以及一資料反混淆處理步驟，依據該第一參數以對該處理器核心由特定位址讀入之資料進行反混淆處理。

由於本發明設計新穎，能提供產業上利用，且確有增進功效，故依法申請發明專利。

〖四、實施方式〗

圖2顯示本發明之一種於處理器中使用位址線對資料進行混淆處理的裝置的示意圖，其中處理器核心200係用以執行處理器之相關指令，並利用位址匯流排210及資料匯流排220來存取記憶體290之資料，前述使用位址線對資料進行混淆處理的該裝置係由種子產生裝置230、第一參數產生裝置240、資料混淆處理裝置250、資料反混淆處理裝置260、選擇裝置271、272及第二參數產生裝置280所構成。

前述種子產生裝置230係耦合至該位址匯流排210，當該處理器核心200使用該位址匯流排210及資料匯流

220排對該記憶體290存取資料時，該種子產生裝置230依據該位址匯流排210上之全部或部分之位址，而以一隨機程序產生而產生一種子。該第一參數產生裝置240係耦合至該種子產生裝置230，以依據該種子產生一第一參數。

該選擇裝置271係耦合至該資料匯流排220，當該處理器核心200欲寫出資料時，該選擇裝置271選擇將欲寫出之資料匯至該資料混淆處理裝置250進行混淆處理，當該處理器核心200欲讀入資料時，該選擇裝置271選擇將該資料反混淆處理裝置260進行反混淆處理後之資料，匯至理器核心200。

該選擇裝置272係耦合至該記憶體290之資料匯流排，當該處理器核心200欲寫出資料時，該選擇裝置272選擇將該資料混淆處理裝置250進行混淆處理後之資料，匯至該記憶體290之資料匯流排，當該處理器核心200欲讀入資料時，該選擇裝置272選擇將欲讀入之資料匯至資料反混淆處理裝置260進行反混淆處理。

該資料混淆處理裝置250係耦合至該選擇裝置271，以當該處理器核心200欲寫出資料至該記憶體290之一特定位址時，依據該第一參數產生裝置240所產生之第一參數而對該資料進行混淆處理。該混淆處理後之資料再經由該選擇裝置272而匯至該記憶體290之資料匯流排。

該資料反混淆處理裝置260係耦合至該選擇裝置272，以當該處理器核心200欲由該記憶體290之一特定位址讀入資料時，依據該第一參數產生裝置240所產生之第一參數而對該記憶體290之資料進行反混淆處理。該反混

淆處理後之資料再經由該選擇裝置271而匯至該處理器核心200之資料匯流排220。

圖3顯示與圖1相同之程式碼，其程式碼事先利用本發明之資料混淆處理裝置250以加密後儲存於一ROM，該段程式碼所儲存的位址係由$1F00_0000_H$至$1F00_0020_H$。其中，該種子產生裝置230之種子(seed)可為位址匯流排210之部分之位址Address[4:2]，亦即該種子為Address[4:2]。第一參數產生裝置240係耦合至該種子產生裝置230，以依據該種子產生一第一參數，本範例中該第一參數產生裝置240可為一對應表，其對應關係如表格1所示，

x	0	1	2	3	4	5	6	7	8
F1(x)	88	60	35	78	60	05	17	25	78

表格1

其中，x為該種子產生裝置230所產生之種子，F1(x)為第一參數產生裝置240所產生之第一參數。故當位址為1F00_0004時，seed=Address[4:2] = 1，第一參數(Parameter1) = F1(1) = 60。上述之第一參數產生裝置240並不只有0~8個欄位，同時該第一參數產生裝置240亦可為其他之對應函數，表格1僅係為舉例說明該第一參數產生裝置裝置240，並不能作為限定該第一參數產生裝置240之依據。

若當該處理器執行到位於1F00_000C之指令#3時，若指令#3為bz $1F00\_0020_H$，此時若根據零旗標(zero flag)

的值，決定該處理器跳躍到1F00_0020$_H$位址處繼續執行，此時該處理器會擷取1F00_0020$_H$位址處所儲存之混淆資料，以完成指令#3之跳躍動作，由於本發明之資料反混淆處理裝置260會對該混淆資料進行反混淆處理，故可得到正確之指令#8，而不會如習知技術中該處理器採用60來對儲存於1F00_0020H位址處之資料做解碼。

雖然該種子產生裝置230係以一隨機程序產生而產生一種子，然而當該處理器核心200欲對位於某一特定記憶體位址之資料進行存取時，該種子產生裝置230係依據該位址匯流排210上之位址而產生一種子，故對同一特定記憶體位址之資料進行存取時，會產生相同之種子，有一對一之關係，並不會產生如圖1中之問題，因此，其不僅可用於ROM的保護，亦能用於如RAM或Flash等隨機讀存記憶體之資料保護。

另為了增加資料混淆處理後的亂度，以免被他人得知該混淆處理的過程，如圖2所示，本發明更以該第二參數產生裝置280以產生一第二參數，而該資料混淆處理裝置250係同時依據該第一及第二參數而進行混淆處理，該資料反混淆處理裝置260係依據該第一及第二參數而進行反混淆處理。

同時為了增加資存取位址的亂度，如圖4所示，本發明更包含一第三參數產生裝置410及一位址混淆處理裝置420以進行位址混淆處理，該第三參數產生裝置410用以產生一第三參數，該位址混淆處理裝置420係耦合至該位址匯流排，當該處理器核心欲對特定位址存取資料

時，其依據該第三參數對該處理器核心之位址進行混淆處理，圖5係圖3中程式碼再以位址混淆處理裝置420對其儲存位址進行混淆處理的結果，由圖5可知儲存在記憶體中的程式碼其前後並無相關性，他人即使擁有該記憶體亦難以讀出真正之程式碼。

由上述之說明可知，本發明之技術由於使用依據存取位址進行資料混淆/反混淆處理，其具有唯一性，故可得到正確之指令或資料，故不僅可用於ROM的保護，亦能用於如RAM或Flash等隨機讀存記憶體之資料保護。

綜上所陳，本發明無論就目的、手段及功效，在在均顯示其迥異於習知技術之特徵，實為一極具實用價值之發明。惟應注意的是，上述諸多實施例僅係為了便於說明而舉例而已，本發明所主張之權利範圍自應以申請專利範圍所述為準，而非僅限於上述實施例。

【五、圖式簡單說明】

圖1：係一程式經由一虛擬亂數產生器依據一初始值進行編碼之示意圖。

圖2：係本發明之於處理器中使用位址線對資料進行混淆處理的裝置之架構圖。

圖3：係圖1之程式經由本發明技術進行編碼之示意圖。

圖4：係本發明之於處理器中使用位址線對資料進行混淆處理的裝置另一實施例之架構圖。

圖5：係圖3之程式經由本發明技術進行儲存位址混淆處理之示意圖。

【圖號說明】

處理器核心	200	位址匯流排	210
資料匯流	220	種子產生裝置	230
第一參數產生裝置	240	資料混淆處理裝置	250
資料反混淆處理裝置	260	選擇裝置	271
選擇裝置	272	第二參數產生裝置	280
記憶體	290		
第三參數產生裝置	410	位址混淆處理裝置	420

拾、申請專利範圍

1. 一種於處理器中使用位址線對資料進行混淆處理的裝置，該處理器具有一處理器核心以執行該處理器之相關指令，並利用一位址匯流排及資料匯流排以存取資料，該裝置包含：

一種子產生裝置，係耦合至該位址匯流排，以依據該位址匯流排上之特定位址而產生一種子；

一第一參數產生裝置，係耦合至該種子產生裝置，以依據該種子產生一第一參數；以及

一資料混淆處理裝置，其耦合至該資料匯流排，以當該處理器核心欲寫出資料至特定位址時，依據該第一參數而對該資料進行混淆處理；以及

一資料反混淆處理裝置，其耦合至該資料匯流排，以當該處理器核心欲由特定位址讀入資料時，依據該第一參數而對該資料進行反混淆處理。

2. 如申請專利範圍第1項所述之裝置，其更包含選擇裝置，用以當該處理器核心欲寫出資料時，選擇將欲寫出之資料匯至該資料混淆處理裝置進行混淆處理，之後再寫至記憶體，而當該處理器核心欲讀入資料時，選擇將欲讀入之資料匯至該資料反混淆處理裝置進行反混淆處理，之後再讀至處理器核心。

3. 如申請專利範圍第2項所述之裝置，其更包含一第二參數產生裝置，以產生一第二參數，該資料混淆處理裝置係依據該第一及第二參數而進行混淆處理，該資

料反混淆處理裝置係依據該第一及第二參數而進行反混淆處理。

4. 如申請專利範圍第1項所述之裝置，其更包含：

一第三參數產生裝置，以產生一第三參數；

一位址混淆處理裝置，其係耦合至該位址匯流排，當該處理器核心欲對特定位址存取資料時，依據該第三參數對該處理器核心之位址進行混淆處理。

5. 如申請專利範圍第1項所述之裝置，其中，該種子產生裝置係依據全部或部分之該位址匯流排上之位址以產生一種子。

6. 如申請專利範圍第4項所述之裝置，其中，該位址混淆處理裝置係依據全部或部分之該位址匯流排上之位址進行混淆處理，以產生一混淆處理之位址。

7. 如申請專利範圍第6項所述之裝置，其中，該位址匯流排上之位址線數目等於該混淆處理後之位址線數目。

8. 如申請專利範圍第6項所述之裝置，其中，該位址匯流排上之位址線數目不等於該混淆處理後之位址線數目。

9. 一種於一處理器中使用位址線對資料進行混淆處理的方法，該處理器包含一處理器核心，該處理器核心係執行該處理器之相關指令，並利用一位址匯流排及第一資料匯流排以存取資料，該方法包含下列步驟；

一種子產生步驟，係依據該位址匯流排上之特定位址以產生一種子；

一第一參數產生步驟，係依據該種子而產生一第一參數；

一資料混淆處理步驟，依據該第一參數以對該處理器核心欲寫出至特定位址之資料進行混淆處理；以及

一資料反混淆處理步驟，依據該第一參數以對該處理器核心由特定位址讀入之資料進行反混淆處理。

10. 如申請專利範圍第9項所述之方法，其中，於該第一參數產生步驟之後更包含一第二參數產生步驟，以產生一第二參數，而使該資料混淆處理步驟係依據該第一參數及第二參數而進行混淆處理，該資料反混淆處理步驟係依據該第一參數及第二參數而進行反混淆處理。

11. 如申請專利範圍第9項所述之方法，其更包含下列步驟：

一第三參數產生步驟，以產生一第三參數；

一位址混淆處理步驟，其係當該處理器核心欲對特定位址存取資料時，依據該第三參數對該處理器核心之位址進行混淆處理。

12. 如申請專利範圍第9項所述之方法，其中，該種子產生步驟係依據全部或部分之該位址匯流排上之位址以產生一種子。

13. 如申請專利範圍第11項所述之方法，其中，該位址混淆處理步驟係依據全部或部分之該位址匯流排上之位址進行混淆處理，以產生一混淆處理之位址。

14. 如申請專利範圍第13項所述之方法，其中，該位址匯流排上之位址線數目等於該混淆處理後之位址線數目。

15. 如申請專利範圍第13項所述之方法，其中，該位址匯流排上之位址線數目不等於該混淆處理後之位址線數目。

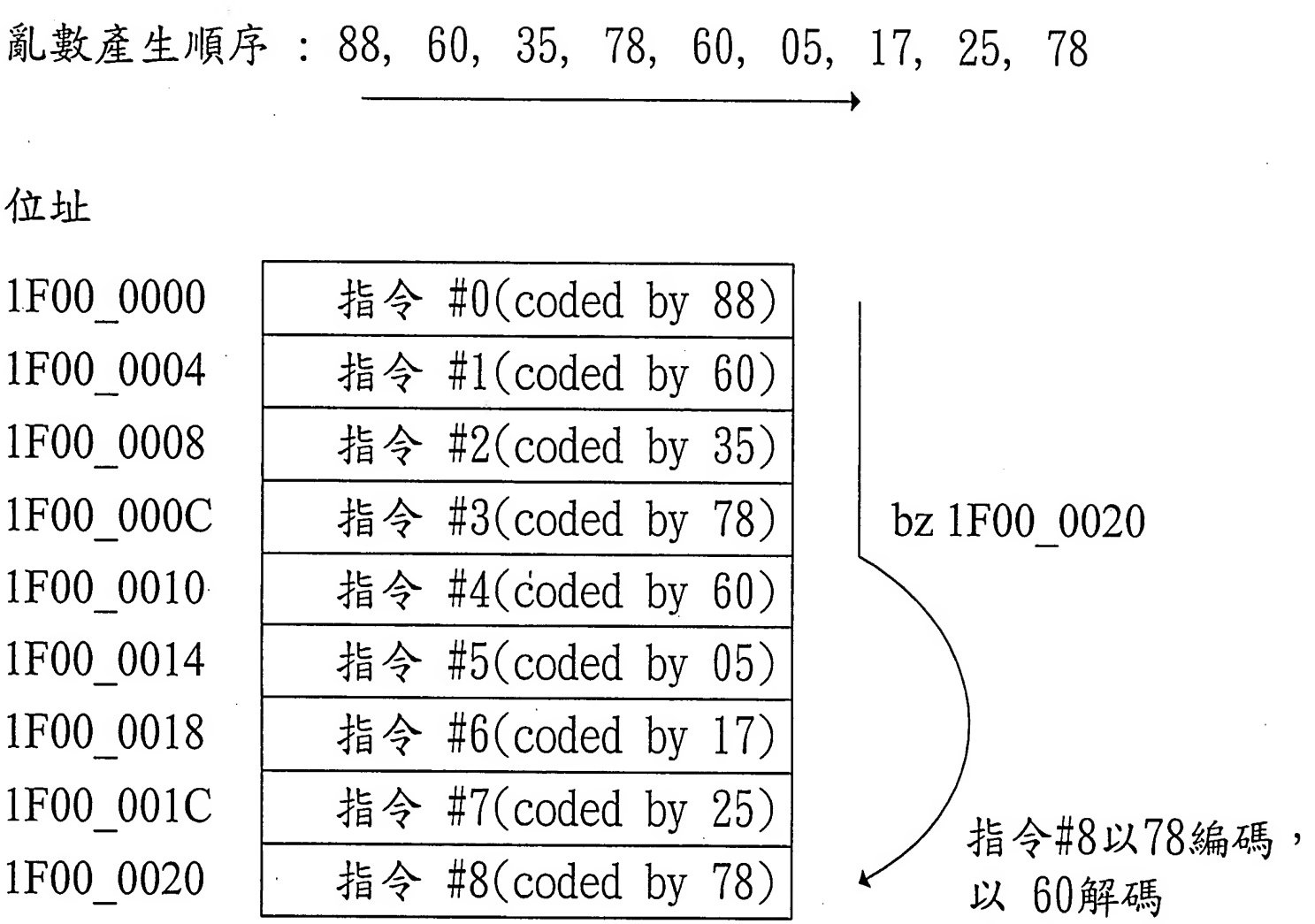
亂數產生順序 : 88, 60, 35, 78, 60, 05, 17, 25, 78
位址
1F00_0000
1F00_0004
1F00_0008
1F00_000C
1F00_0010
1F00_0014
1F00_0018
1F00_001C
1F00_0020
指令 #0(coded by 88)
指令 #1(coded by 60)
指令 #2(coded by 35)
指令 #3(coded by 78)
指令 #4(coded by 60)
指令 #5(coded by 05)
指令 #6(coded by 17)
指令 #7(coded by 25)
指令 #8(coded by 78)
bz 1F00_0020
指令#8以78編碼，
以 60解碼

圖 1

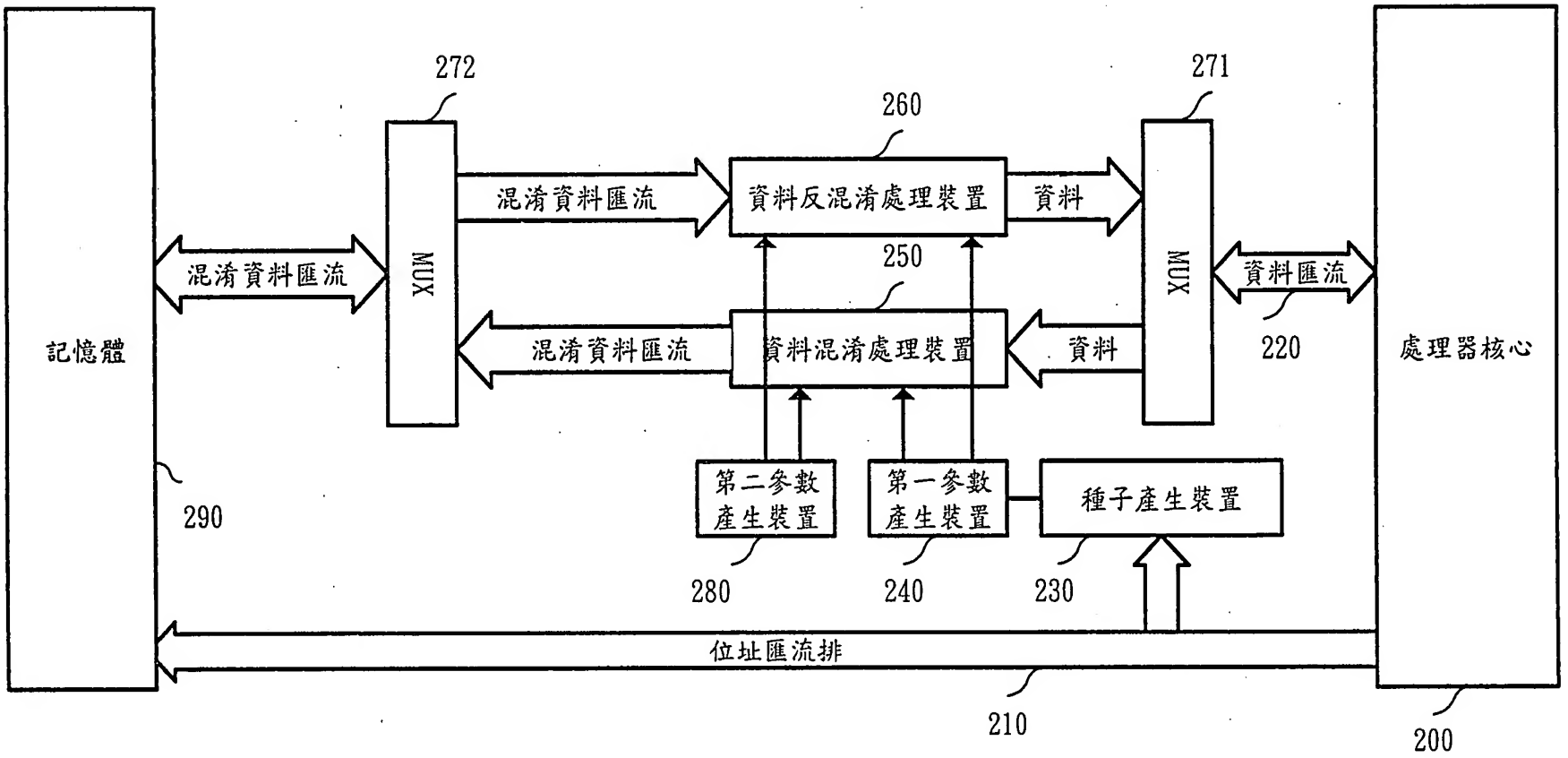
記憶體
290
混淆資料匯流
272
MUX
混淆資料匯流
260
資料反混淆處理裝置
資料
271
MUX
資料匯流
220
處理器核心
200
250
資料混淆處理裝置
混淆資料匯流
資料
第二參數
產生裝置
280
第一參數
產生裝置
240
種子產生裝置
230
位址匯流排
210

圖 2

由位址產生之種子: 88, 60, 35, 78, 60, 05, 17, 25, 78

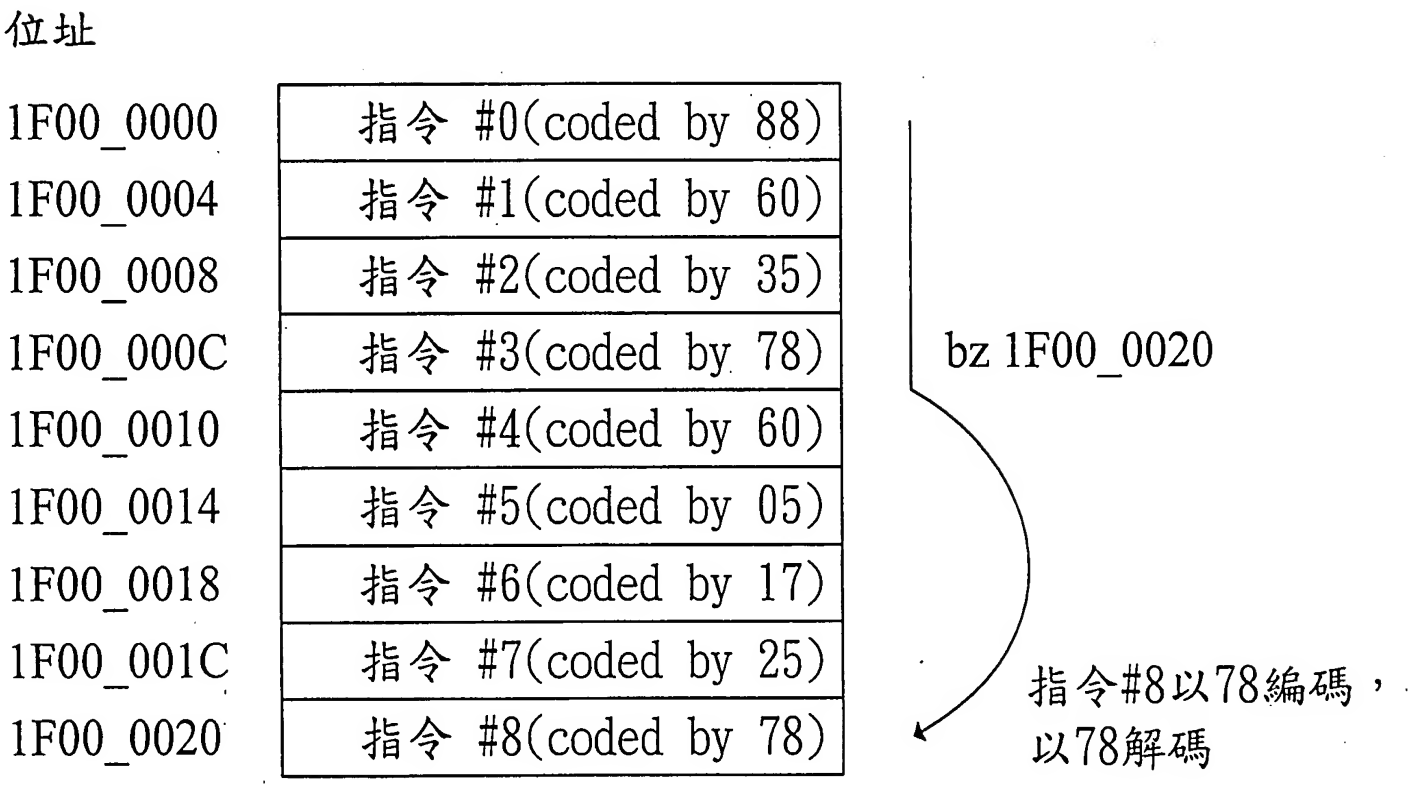

圖 3

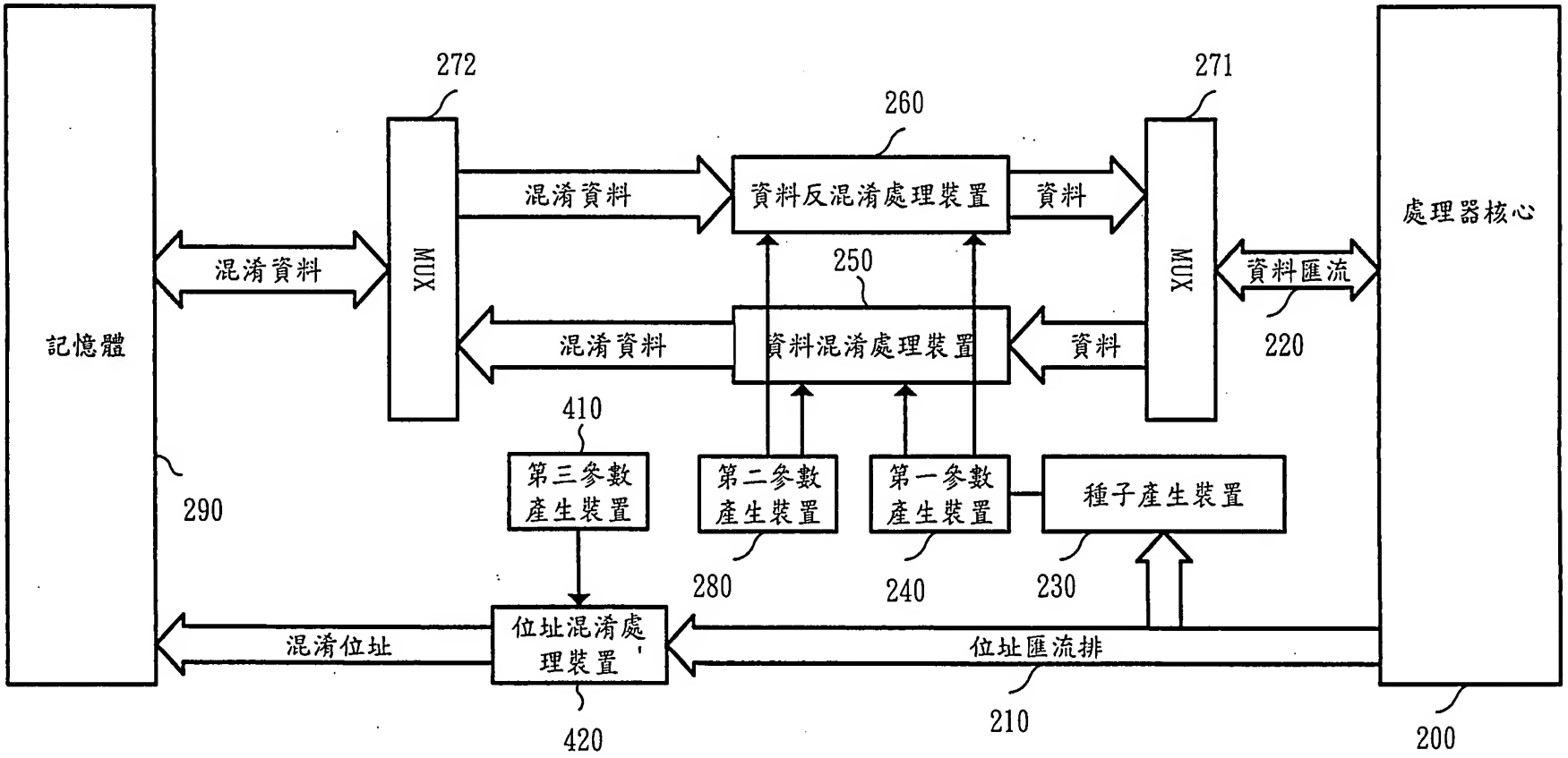
記憶體
290
272
MUX
混淆資料
混淆資料
260
資料反混淆處理裝置
混淆資料
資料
271
MUX
處理器核心
資料匯流
220
250
資料混淆處理裝置
資料
410
第三參數
產生裝置
第二參數
產生裝置
第一參數
產生裝置
種子產生裝置
280
240
230
位址混淆處
理裝置
混淆位址
位址匯流排
420
210
200

圖 4

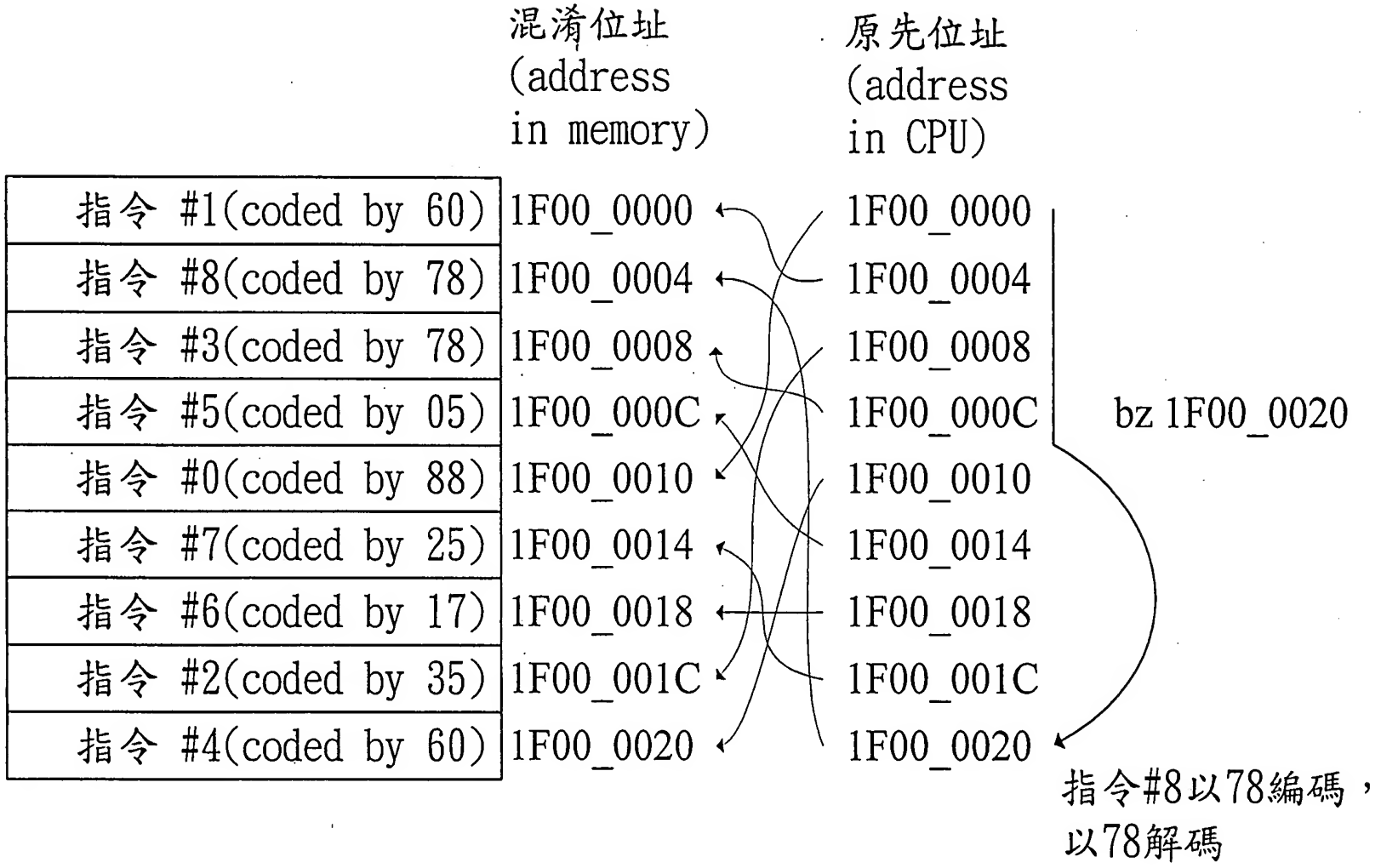
混淆位址
(address
in memory)
原先位址
(address
in CPU)
指令 #1(coded by 60)
指令 #8(coded by 78)
指令 #3(coded by 78)
指令 #5(coded by 05)
指令 #0(coded by 88)
指令 #7(coded by 25)
指令 #6(coded by 17)
指令 #2(coded by 35)
指令 #4(coded by 60)
1F00_0000
1F00_0004
1F00_0008
1F00_000C
1F00_0010
1F00_0014
1F00_0018
1F00_001C
1F00_0020
1F00_0000
1F00_0004
1F00_0008
1F00_000C
1F00_0010
1F00_0014
1F00_0018
1F00_001C
1F00_0020
bz 1F00_0020
指令#8以78編碼，
以78解碼

圖 5